Assessing Identity and Access Management Systems Based on Domain-Specific Performance Evaluation

Frank Schell, Andreas Schaf, Jochen Dinger, and Hannes Hartenstein

{frank.schell|andreas.schaf|jochen.dinger|hannes.hartenstein}@kit.edu
Steinbuch Centre for Computing, Karlsruhe Institute of Technology, Germany

Categories and Subject Descriptors

C.4 [**Performance of Systems**]: Design studies; D.2.8 [**Software Engineering**]: Metrics—*performance measures*

General Terms

Design, Performance, Security

1. INTRODUCTION

Identity and access management (IAM) assures authorized access to services, particularly in highly distributed environments like service-oriented architectures (SOA). Corresponding IAM systems are often highly distributed systems themselves because the components are also distributed within the overall system environment. Hence, various design decisions have to be made for an appropriate system architecture, in particular the question of where to position IAM-related components in such a distributed environment. For example, SOA enables outsourcing of authentication, authorization, provisioning, and user data that is necessary for access control. Thereby, user data is not controlled centrally, but might be distributed over a number of services that control user attributes, e.g., an HR service is authoritative for first name and given name of employees, and an IT department is responsible for e-mail addresses. One the one hand, this improves data quality by reducing the number of distributed and (possibly) outdated user information. On the other hand, performance might be decreased, due to additional service calls and failures at runtime. Furthermore, the distribution of user data to several information providers raises the risk of bottlenecks, e.g., services that aggregate user data from several integrated and distributed services, at peak times. To support the making of fundamental design decisions for complex architectures qualitative measures for the evaluation of different IAM systems have been presented in [3] and [6]. Based on our work in [5] we now extend this evaluation by proposing a framework for the quantitative analysis of IAM architectures on a simulative basis even before deploying IAM systems.

2. IAM SYSTEM MODEL

To analyze performance issues of IAM systems a corresponding model has to consider several aspects, i.e., behavior, delays, and failure rates of system components, IAM system architecture, network connectivity, and user behavior. Hence, to model different IAM systems we identified several system components in [5] as shown in Fig. 1. These components may be combined to simulate and evaluate the overall IAM processes of different IAM architectures as it is depicted for the IAM system Shibboleth [7] in Fig. 2. Furthermore, each IAM component can be instantiated with a specific behavior, e.g., an authentication provider only authenticates users or also aggregates user attributes. This behavior and network properties for each connection between system components allow the specification of characteristic delays and failure rates. Thus, we are able to model local, federated, or even global IAM systems by specifying the bandwidth and delay of specific channels. In addition, the user model has significant impact on the overall performance of IAM systems, due to the differences in user load, number and kind of service calls in a session, preferred authentica-

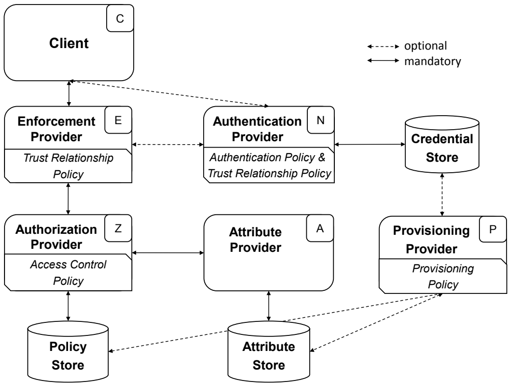

Figure 1: IAM System Components and IAM System Policies at a Glance

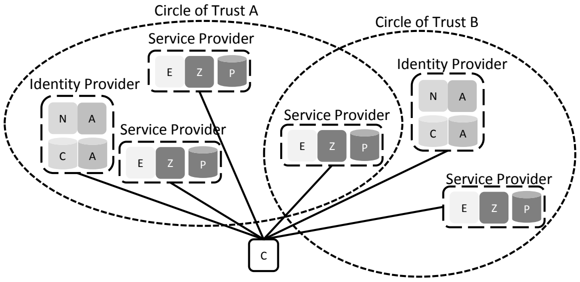

Figure 2: IAM Model Instance of Shibboleth

WOSP/SIPEW'10, January 28–30, 2010, San Jose, California, USA.
ACM 978-1-60558-563-5/10/01.

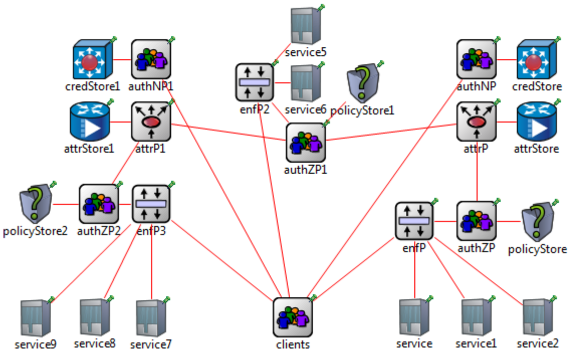

Figure 3: Example of Shibboleth in OMNeT++

tion mechanisms, trusted authentication providers, and user attributes that are available for an IAM system.

3. SIMULATIVE EVALUATION OF IAM

The goal of a simulative evaluation based on our IAM system model is to support the non-trivial task of making design decisions. Therefore, we define the metric for performance as the delay of an IAM system calculated at enforcement providers as these are the entry points for each service request. For this reason, this metric covers the overall access control process from an initial service request at an enforcement provider over the authentication provider call to the authorization decision request at the authorization provider. However, the performance evaluation of IAM systems is not only limited to the measurement of delays. Hence, the authors of [1] present identity management risk metrics for decision support in risk reporting, predictive modeling, and real-time decision making. Moreover the authors of [2] propose a comprehensive approach called *Identity Analytics* for simulating and evaluating IAM systems. They focus on the prediction of operational costs, reputation, compliance etc. to give support in deciding on new or existing IAM investments. We also identified additional domain-specific performance metrics that aim at the evaluation of IAM architectures, e.g., accuracy of access control as the number of decisions based on wrong or outdated user information, work load of single components, and privacy issues like the number of provided user attributes to other organizations and components. To identify relevant parameters for the determination of IAM architectures we use the open source simulation framework OMNeT++ [8] that provides the flexibility to implement the proposed system model and metrics. A specific IAM architecture can be configured in OMNeT++ using predefined modules and channels as it is depicted in Fig. 3. The figure shows an exemplary Shibboleth-based IAM architecture as an instance of our model. The deliverables of such model instances help system architects to determine a fitting IAM architecture by evaluating and comparing consequences of different design decisions with the stated requirements of their specific project. An exemplary evaluation of 2 different Shibboleth-based instances of our IAM system model is depicted in Figure 4. In this scenario Shibboleth using local access control decision components surpasses Shibboleth using a centralized policy decision point – e.g. a system based on Shibboleth for authentication and PERMIS [4] for authorization – w.r.t. response time. However, as a basis for evaluating IAM instances on a simulative basis we need input distributions, e.g., user interarrival times and service times. Currently, we empirically determine distributions for different aspects like user behavior, i.e., user arrival times, changes of user attributes, and number of service calls in a session, in a federated IAM project at the Karlsruhe Institute of Technology (KIT) to model IAM instances with these properties.

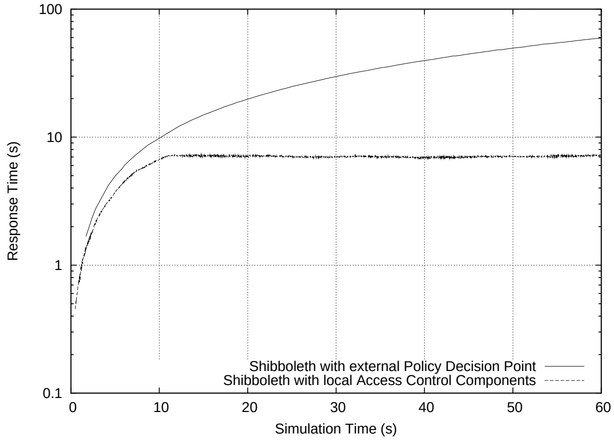

Figure 4: Exemplary Evaluation of 2 Shibboleth-Based Scenarios

4. CONCLUSIONS AND FUTURE WORK

In this contribution we proposed a framework for IAM that can be used to evaluate different system-design decisions, in particular the positioning of components. This approach helps system architects to investigate and determine adequate design decisions and to find a fitting system instance that serves the needs of their specific use case best. Accordingly, we sketched an IAM model and showed an implementation of our model with the open source framework OMNeT++. Besides supporting the design of new IAM systems that are built from scratch, our work can also be used to analyze the effectiveness of planned improvements in advance. Next steps include the refinement of the presented model and metrics.

5. REFERENCES

[1] G. Peterson. Introduction to identity management risk metrics. *IEEE Security and Privacy*, 4(4):88–91, 2006.

[2] M. Mont, A. Baldwin, and S. Shiu. On identity analytics: Setting the context. HP technical report, HPL-2008-84, 2008.

[3] T. Höllrigl, F. Schell, S. Suelmann, and H. Hartenstein. Towards systematic engineering of service-oriented access control in federated environments. In *IEEE Congress on Services Part II, SERVICES-2*, pp. 104–111, 2008.

[4] PrivilEge and Role Management Infrastructure Standards (PERMIS). http://sec.cs.kent.ac.uk/permis, 2009.

[5] F. Schell, J. Dinger, and H. Hartenstein. Performance evaluation of identity and access management systems in federated environments. In *Proc. of the 4th Int'l ICST Conf. on Scalable Information Systems. Infoscale'2009*, 2009.

[6] C. Schläger and M. Ganslmayer. Effects of architectural decisions in authentication and authorisation infrastructures. In *Proc. of the 2nd Int'l Conf. on Availability, Reliability and Security. ARES'2007*, pp. 230–237, 2007.

[7] Shibboleth. http://shibboleth.internet2.edu, 2009.

[8] OMNeT++. http://omnetpp.org, 2009.